ACCELERATING CRYPTOGRAPHIC HASH COMPUTATIONS

ABSTRACT OF THE DISCLOSURE

Provided is an apparatus and method for accelerating cryptographic hash computations. For example, in a cryptographic hash computation such as SHA-1, multiple execution units in a processor can process loosely coupled data. Specifically, after preprocessing a message with a particular bit length and parsing the padded message into multiple blocks, a first execution unit can begin processing the blocks for a message schedule computation. While the first block is processed, the first execution unit produces a partial result for the computation of the compression function in the second execution unit. By simultaneously processing the blocks on multiple execution units, the cryptographic hash computation performance can improve.